REMINDER: **Emailed to a group account. Do NOT reply using email group account.**
For comments or inquiries email infosec@pjlhuillier.com.

May 10, 2013 Release # 214

-- Begin Transmission --

Top 10 Social Engineering Tactics – Part 4

Top 10 Social Engineering Tactics – Part 4

5. Catch Me a Vish

Not having much success with phishing or whaling? Try vishing! Vishing is an attack that uses telephone to perform the equivalence of a phishing attack.

A common and effective example is using a war dialler. It is a computer program that is used to identify the phone numbers that can successfully make a connection with a computer modem. The program automatically dials a defined range of phone numbers and logs and enters in a database those numbers that successfully connect to the modem. A war dialler is typically used by a hacker to identify potential targets. If the program does not provide automated penetration testing, the intruder attempts to hack a modem with unprotected log-ins or easily cracked passwords. Such modems can provide easy access to a company's intranet.

Another popular variation of a vishing attack is sending the original message through a text message to a cell phone instead of calling the person directly.

4. Social (Engineer) Networking

Social networking sites such as Facebook and MySpace are a social engineer's paradise. A social engineer can find out so much about you from these sites. People post information about where they work, what they like to do, what bands they like, and more. A social engineer can use the information being posted on the social networking page in a number of ways:

- Sending an email impersonating a friend listed on the page asking for confidential information.
- Viewing pictures of a person to find out popular hang-outs and then showing up at the same spots to social-engineer the person outside of a work environment.
- Discovering the person's age, place of birth, school, and previous companies, which can all be used to target the person in a spear phishing attack.
- Adding the person as a friend to build up an online relationship with a person in order to build trust. The social engineer then exploits that trust to get information from the person which could be used to launch another attack.

…to be continued

-- End of Transmission --

Information Security: It's a Shared Responsibility
REFERENCE(S): http://www.informit.com/
http://searchsecurity.techtarget.com/definition/war-dialer

INTERNAL USE ONLY: For circulation within the PJ Lhuillier Group of Companies only.